中美网络大战——网络战争向我们走来

http://jczs.sina.com.cn 2001年5月12日 09:44

沙林

双方违法的中美黑客大战

5月1日，中美黑客大战开始。中华少年壮士很激奋，8万黑客红客狂攻白宫，无数中美网站被黑掉。虽然没有一个人死，也没有人流血，但由中美撞机事件引发的中美黑客大战却吸引了无数眼球。、

也许是凑巧，此时，一本名叫《网络战争》的书正好面世。其作者国防大学军事科技与装备教研室主任张召忠教授虽然没预见到这次黑客大战，但玩过6台计算机的他却忍不住对此大战"点评"一番：

这次中美黑客大战，在网络战中是最低层次的，或许根本算不上网络战。我们的黑客用的最多的战术是阻塞攻击，即用大容量去阻塞美方的线路。但这种阻塞不会造成对方什么损失，顶多导致暂时的瘫痪。还有常用的手法是删改对方的页面，写上"打倒美帝国主义"等句子。

但我们所能攻击到的都是对方在不设防的因特网上供一般民众了解政府用的宣传的网站。真正的军方网站没有黑掉一个。我所知道就是一个美海军供通讯用的也属民用的网站被黑。而且这些被黑的网站都在几分钟之内或是一两个小时之内自动恢复了正常。

这且不论，重要的是这种做法是错误的，不管是中国黑客还是美国黑客，不管是谁先动手，即使我们黑掉的是白宫，这种做法也是错误的。因为根据战争法中的"目标区分原则"，在战争或敌对国家之间，攻击非军事目标是非法的。

这次主要是中国黑客联盟、中国红客联盟、鹰派三大黑客组织，他们振臂一呼，全国响应。他们报效国家的热情是好的，绝对需要肯定，但仗不是这么打的，这在国际上给中国黑客带来了负面影响。因为中国上去狂轰的人数太多，一种锱铢必较的仇恨原则在普及。

对于黑客，我们一定要正视，能当黑客的绝对是聪明人，最可贵的是他们有责任感，这帮小子日夜奋战，无酬无薪，无怨无悔。以后为了维护国家的网络安全还得靠他们。我们国家早晚要成立一支网络部队，就像时候到了，要成立一支战略导弹部队二炮一样。从哪儿招募兵勇，农村扛锄头的肯定不行，还得从这些人中挑选。

能像关电灯一样"关掉美国"吗

初级黑客大拼比不算网络战，那网络战是什么呢？

张召忠在《网络战争》一书很鄙视以下的观点。他说，我们许多文人以及舆论界心目中的网络战或是信息战是什么样呢，似乎发掘一个聪明绝顶的少年，外加一台电脑，一个调制解调器，一条电话线，就足以发动一场令人心惊胆战的信息进攻。

有人断言，美国现在倾其国力在发展信息高速公路，让它搞去好了，我不必搞那玩意儿，只需发展黑客就行了。信息和网络越先进，就越脆弱，就越经不起打击。你给我10亿美元外加20个能力高强的黑客，就可以像关掉一台计算机那样“关掉美国”。在这些人眼里，美国真成了“纸老虎”，只要你历尽千辛万苦带个火种过去，就足以把这个纸老虎给焚毁。

张召忠认为，这是美国人的宣传，我们拿过来就用，是受了美国人的骗了。

网络战争有许多是炒作的成分，是媒体的作用，比如千年虫，前一段时间闹得沸沸扬扬，实际有什么千年虫？全都受骗了！专家的作用就是要在这混钝之中排疑解惑。

张召忠自恃上个世纪80年代中期就有玩计算机的功底，认为说美国能够像关电灯一样被关掉的人根本不懂网络，说话不负责任。他说，最起码在30年之内，我们看不到传统武器的终期，因而我们还要非常重视传统火力战。不能说机械化不搞了，就搞网络战，在没有传统工业的土地上搞所谓网络战争，结果将是两者都没捞到。

那些认为可以不要传统武器的人以为，大众都能进去的不设防的因特网就是网络的全部，攻击了它就能取得决定性的胜利。实际稍微关键一些的部门，就非常难进了，这次中美黑客大战，中方黑客没有进到任何一个关键性的网站里就是这个道理。你不要以为上了别人的网络，就可以肆无忌惮地到处乱窜，各个网络都设有自己的防火墙，要想越过这些防火墙，你先得准备剥层皮，丢条命。

最关键的是，美国军方网络与因特网是绝缘的，跟因特网没有物理联结。你想从你自己的电话线上去攻击它，简直如水中捞月。

这将不再是科幻电影

咱们先体会一下张召忠给我们描述的网络战争的一种吧。真正可怕的力量藏在局域网中。网络战争最大的动力也来自局域网。这是一种美国人就要实现了的或者说已经实现了的类似于科幻电影中的来自宇宙深处的舰队集群。它可能是全新的战争平台，如人类从未见过的充满可怖武器的数字飞行平台，或者就是被网络联结的普通坦克、军舰、甚至士兵。

张召忠给我们描述了一种最普通的网络战图景：数字化网络把独立作战的坦克连接到一起，构成坦克连级战术分系统，通过战区区域网络构成坦克营级分系统，再通过全球指挥控制网络组合成坦克旅级、师级或军级分系统，进而与其他军兵种的所有分系统相连，最终形成一个四通八达的自动化信息网络系统。这样的战场数字化网络，起码实现了三大革命：一是横向一体化。数字网络把一辆辆分散的战车连在一起，形成了可怕的武库集群。你想像，当上千辆坦克都准确无误地向一个或两个目标轰击时，什么东西还能完好无损?

二是射手的高度准确性，当电子侦察部队发现目标后，可将目标的数据、图像等信息直接传输给武器射手，对目标实行精确打击。

三是协同作战。当坦克集群在纵深突破时如遇到敌人装甲部队强火力拦阻，该坦克群可直接将目标参数通报给海军或空军，召唤远程精确打击。特殊情况下，坦克集群还可通过全球指挥控制网络系统直接调用海军舰艇上的远程导弹对目标进行攻击。

总之，这是一个高度数字化的作战图景。一个指挥员可以命令空中、陆上、海上、甚至空间武器去攻击敌人目标，目标信息会从卫星或无人飞机上直接传送给士兵。

这就是美国一直在追求的C4ISR系统，也是作为军事科技与装备专家的张召忠所强调我国应该借鉴的。

他说，鉴于网络战的前景和实际，在全军武器装备发展的排序中，应当尽快转变那种重平台、轻负载的传统落后观念，即只重视传统的坦克、战车、火炮、军舰，而不重视这些传统平台所负载的导弹、计算机控制、侦察定位系统的做法，切实把C4ISR装备放在首位。

在装备的研制上也不必求全，而应自己研制一些关键性的高精尖武器。老一代的领袖和军事家在这方面给我们作出了榜样。五六十年代，我们被充满敌意的国家包围，海陆空三军的武器均落后于人。加上3年困难时期，全国人民勒着肚皮，就这么一点钱，发展什么呢？老一代领导人一眼就盯准了两弹一星，事实证明，有了这些，整体的军事力量对比马上改观。

一个军人的忧虑

除了基于传统武库的C4ISR系统外，网络战争还有另外的形式，这可能比较接近人们想象中的网络战。

张召忠举出了几例：比如施放高能微波炸弹，能在方圆几十公里使网络和计算机失灵，使电脑中的所有的记忆永远消失，永难恢复。这种高能微波炸弹可用小型飞机偷运到敌国上空引爆，也可采取恐怖主义的办法，在城市当中起爆。

引发极为厉害的电脑病毒也是战法之一。这是一种比台湾的陈盈豪发明的病毒还要厉害得多的一种毁灭性病毒，它可以吞噬芯片。

还有一种网络战法为美国独有的。这就是利用因特尔和微软在设计软硬件时留下的“后门”，随时进入敌方的指挥中心的芯片和硬件中，去扰乱或摧毁敌国要害。

视窗98和视窗2000在出产时都有序列号，就像一辆汽车一样，都打上了钢印，人们有理由相信，美国中情局或者军方理所当然地会利用这些序号，以便跟踪(这在电脑行业规范中是不允许的)芯片和电脑的去处，进行遥控和破坏。而中国去年就引进了800亿元人民币的美国电脑和计算机元件，今年将达到1000亿元。

这是没有办法的办法，我们不能像俄罗斯那样，在电脑上搞闭关锁国———世界上哪个国家都发现了电脑病毒，比如日本、美国、欧洲各国等，就是俄罗斯没有，因为在计算机方面，它是自己弄不出来宁愿不用，就是不用别人的。不用美国的芯片，哪来的美国的病毒？

张召忠说到这就有些痛心疾首了：一般民用商用还没事，关键部门、军事指挥部门用的电脑芯片还是因特尔的，难道我们就那么放心吗？好在我们这一两年正在加紧发展，估计不久的将来就可以满足关键部门的芯片之需。

作为军人，国家安全在张召忠的心里始终是最重要的。

【军事论坛】【关闭窗口】

首页 | 将军寄语 | 中 国军事 | 军事图片 | 武器纵横 | 国际风云 | 周边军情 | 战略视角 | 各国军力